Docket No.: D2538 PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| In re Application of | : | Customer Number: 000043471 |
| Alexander Medvinsky | : | Confirmation Number: 8249 |
| Application No.: 09/765,108 | : | Tech Center Art Unit: 2136 |
| Filed: January 16, 2001 | : | Examiner: Carl G. Colin |

For: METHOD FOR SECURELY COMMUNICATING INFORMATION PACKETS

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

## BRIEF ON APPEAL

### (1) Real Party in Interest

The real party in interest is Motorola, Inc.

### (2) Related Appeals and Interferences

None.

### (3) Status of Claims

Rejected Claims

1-7 and 10-23.

Canceled Claims

8 and 9.

Claims Appealed

1-7 and 10-23.

**(4) Status of Amendments**

The amendment filed on September 18, 2006, in response to the Office Action dated May 23, 2006 was entered by the Office Action dated November 21, 2006.

**(5) Summary of Claimed Subject Matter**

1. (Previously presented) A system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system comprising:

a local multimedia terminal adapter receiving the voice packets having a time stamp synchronization source operable to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter, the local multimedia terminal adapter comprising, (*See e.g.*, Application at page 8, lines 4-12; page 8, lines 22-28; and FIG. 1)

a local key stream generator for generating a first key stream; (*See e.g.*, Application at page 6, lines 19-20; page 7, lines 17-18; and FIG. 1)

a packet encryptor that encrypts the voice packets using at least a portion of the first key stream to form encrypted voice packets; (*See e.g.*, Application at page 7, lines 15-16; page 8, lines 7-8; and FIG. 1)

the remote multimedia terminal adapter receiving the encrypted voice packets, the remote multimedia terminal adapters further comprising, (*See e.g.*, Application at page 4, lines 29-31; page 8, lines 16-18; and FIG. 1)

a remote key stream generator for generating the first key stream in order to decrypt the encrypted voice packets; (*See e.g.*, Application at page 7, lines 19-22; page 8, lines 16-21; and FIG. 1) and

a packet decryptor decrypting the encrypted voice packets using the first key stream, wherein both key stream generators generate a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session and the packet encryptor and packet decryptor use the second key stream. (*See e.g.*, Application at page 8, lines 22-28; page 9, lines 7-11; page 10, lines 3-23; and FIGS. 1 and 2)

6. (Previously presented) A system for communicating Real Time Protocol voice packets

between a local and a remote location over an Internet protocol network, the system comprising:

a stream cipher module for encrypting the voice packets; (*See e.g.*, Application at page 5, lines 3-6; page 8, lines 7-8; page 8, lines 13-21; and FIG. 1) and

a key stream generator for generating a first Real Time Protocol key stream, the stream cipher module employing the first key stream to encrypt the voice packets for forwarding to the remote location, the key stream generator producing a second Real Time Protocol key stream for encrypting the voice packets when the system switches from a first communication parameter to a second communication parameter, each of the first and second parameters being involved in the synchronization of the key stream, wherein the voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local and remote locations. (*See e.g.*, Application at page 5, lines 6-10; page 8, lines 6-21; page 8, lines 25-29; page 9, lines 7-11; page 10, lines 3-19; and FIGS. 1 and 2)

13. (Previously presented) A method for securely transmitting Real Time Protocol voice packets from a local to a remote location via a communication network, the method comprising:

generating a first Real Time Protocol key stream for encrypting the voice packets; (*See e.g.*, Application at page 5, lines 11-14; page 6, lines 19-20; page 7, lines 17-18; and FIG. 1)

forwarding encrypted voice packets to the remote location; (*See e.g.*, Application at page 5, lines 13-14; page 8, lines 16-18; and FIG. 1)

generating a second Real Time Protocol key stream for encrypting the voice packets in response to a request to change communication parameters for the same media stream during a communication session; (*See e.g.*, Application at page 5, lines 14-17; page 9, line 7 to page 10, line 29; and FIGS. 1 and 2) and

forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location, wherein the voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local and remote locations. (*See e.g.*, Application at page 5, lines 14-17; page 8, lines 6-21; page 8, lines 25-29; and FIG. 1)

17. (Previously presented) In a communication system having a gateway receiving communication sessions from two or more multimedia terminal adapters, a method for securely exchanging voice packets between the multimedia terminal adapters and the gateway, the method

comprising:

generating a first Real Time Protocol key stream for encrypting the voice packets; (*See e.g.*, Application at page 5, lines 21-23; page 6, lines 19-20; page 7, lines 17-18; and FIG. 1)

forwarding the voice packets encrypted with the first Real Time Protocol key stream to the gateway; (*See e.g.*, Application at page 5, lines 21-23 and FIG. 1)

generating a second Real Time Protocol key stream for encrypting the voice packets during a communication session in response to a collision detection wherein the multimedia terminal adapters have the same source identifier; and (*See e.g.*, Application at page 5, lines 23-27; page 6, lines 24-27; page 10, lines 24-33; and FIGS. 1 and 2)

forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location, wherein the voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local multimedia terminal adapter and remote multimedia terminal adapter. (*See e.g.*, Application at page 5, lines 23-27; page 8, lines 6-21; page 8, lines 25-29; and FIG. 1)

19. (Previously presented) A system for securely transmitting voice packets during a communication session from a local location to a remote location over a communication network, the system comprising:

a means for generating a first key stream at the local location; (*See e.g.*, Application at page 5, lines 28-31; page 6, lines 19-20; page 7, lines 17-18; and FIG. 1)

a means for encrypting the voice packets using at least a portion of the first key stream to form encrypted voice packets; (*See e.g.*, Application at page 5, lines 30-32; page 7, lines 15-16; page 8, lines 7-8; and FIG. 1)

a means for forwarding the encrypted voice packets from the local location to the remote location; (*See e.g.*, Application at page 5, line 32 to page 6, line 1; and FIG. 1)

a means for generating the first key stream at the remote location in order to decrypt the encrypted voice packets; (*See e.g.*, Application at page 6, lines 1-2; page 7, lines 19-22; page 8, lines 16-21; and FIG. 1) and

a means for decrypting the encrypted voice packets using the first key stream, wherein both means for generating are capable of generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session, wherein the

voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local and remote locations. (*See e.g.*, Application at page 6, lines 2-4; page 8, lines 22-28; page 9, lines 7-11; page 10, lines 3-23; and FIGS. 1 and 2)

**(6) Grounds of Rejection to be Reviewed on Appeal**

A. The rejection of claims 1-3, 6, 7, 10-16, and 19-23 as being unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Number 5,940,508 ("Long") in view of U.S. Patent Number 5,081,679 ("Dent").

B. The rejection of claims 17 and 18 as being unpatentable under 35 U.S.C. § 103(a) over Long in view of Dent, and further in view of U.S. Patent Application Publication Number 2002/0031126 ("Crichton").

**(7) Argument**

The Final Office Action has failed to establish a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness, three basic criteria must be met:

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

MPEP § 2143. Appellant respectfully submits that the proposed combination of the cited prior art fails to describe or suggest all the limitations of independent claims 1, 6, 13, 17, and 19. The following remarks first address the improper rejection of independent claims 1, 6, 13, and 19; then address the improper rejection of dependent claims 2, 7, and 20; and finally address the improper rejection of independent claim 17.

A. Long and Dent, in the proposed combination, fail to describe or suggest all the features of independent claims 1, 6, 13, and 19, and therefore fail to render obvious these claims along with their dependent claims

Claims 1, 6, 13, and 19, along with their dependent claims 2, 3, 7, 10-12, 14-16, and 20-23 were rejected as being unpatentable over Long in view of Dent. Appellant respectfully requests reversal of this rejection for at least the following reasons.

Claim 1 recites a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network. The system includes a local multimedia terminal adapter receiving the voice packets having a time stamp synchronization source operable to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter. The local multimedia terminal adapter includes a local key stream generator for generating a first key stream, and a packet encryptor that encrypts the voice packets using at least a portion of the first key stream to form encrypted voice packets.

The remote multimedia terminal adapter receiving the encrypted voice packets. The remote multimedia terminal adapters further includes a remote key stream generator for generating the first key stream in order to decrypt the encrypted voice packets and a packet decryptor decrypting the encrypted voice packets using the first key stream. Both key stream generators generate a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session and the packet encryptor and packet decryptor use the second key stream.

Appellant respectfully requests reversal of the above-stated rejection because the proposed combination of Long and Dent fails to describe or suggest a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system including, among other features, a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1.

Long discloses a method and an apparatus for seamlessly changing a key of a cryptosystem. Long at col. 1, line 65 to col. 2, line 2. Referring to FIG. 1 of Long, the cryptosystem includes an encryptor equipment (10) and a decryptor equipment (20). Long at col. 2, lines 4-8. Data to be made secure over a communication link by coding is entered into the encryptor equipment (10), where the data is encrypted, and the encrypted data is then sent to the decryptor equipment (20), where the data is decrypted. *Id.* Referring to FIG. 2 of Long, the encryptor and decryptor equipments (10, 20) each includes a module 2 adder/exclusive OR function (90), a key generator ("KG") (80), a bank of key variables (70), a key multiplexer (50), a KG clock counter (30), and a comparator (60) to control the multiplexer (50). Long at col. 2, lines 21-42.

In operation, the encryptor and decryptor equipments (10, 20) are each loaded with two KG

variables (70) (e.g., key variable 1 and key variable 2). Long at col. 2, lines 43-44. Thereafter, a switchover value is loaded into the switchover comparison register (60) and the KG clock counter (30) counts KG clock states. Long at col. 2, lines 48-50. When the KG clock counter (30) reaches a specified switchover value (checked by the comparator (60)), the key multiplexer (50) switches from key variable 1 to key variable 2 (70). Long at col. 2, lines 52-55. In this manner, both encryption equipments (10, 20) perform the switchover at the same KG state because the switchover is based on KG clocks, and not based on time or other control operations. Long at col. 2, lines 56-60.

Toward this end, Long describes generating a second key when the key generator clock counter reaches a particular switchover value, and it does not describe generating a second key steam when a *component used to transmit the Real Time Protocol voice packets changes* during the communication session, as recited in claim 1. For example, Long does not describe or otherwise suggest generating a second key stream when a first coder/decoder for compressing/decompressing the voice packets changes to a second coder/decoder, as recited in claim 2. For another example, Long does not describe or otherwise suggest generating a second key stream when a Message Authentication Code algorithm changes, as recited in claim 3.

As such, Long fails to describe or suggest a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system including, among other features, a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1.

Not only Long fails to describe the above-recited feature of claim 1, but it also teaches away from it. That is, Long expressly teaches away from generating a second key stream using other control options. *See e.g.*, Long at col. 2, lines 57-60 (stating "[b]oth encryption equipments, 10 and 20, perform switchover at exactly the same KG state because the switchover is based on KG clocks, and *not based on time or other control options*"). In response to the Appellant's previous arguments, the Examiner incorrectly interprets the above-recited feature of claim 1. In particular, the Examiners interprets the recitation "when a component used to transmit the Real Time Protocol voice packets changes" of claim 1 as "a parameter that changes in the transmission of packets," and relies on column 4, lines 30-35 and lines 53-56 of Long to show the alleged interpretation. Appellant disagrees with the Examiner.

In the relied upon portions, Long teaches switching, when the counter reaches the specified value, a multiplexer for both an encrypting and decrypting subsystems from a first key variable to a second key variable. This, without more, does not suggest that the changing counter is used in the transmission of the packets. Accordingly, Long fails to describe or suggest a system that includes, among other features, a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1.

Dent describes a system for the synchronization of encryption and decryption in a duplex cellular radio system in which an encrypted call may be switched from one cell to another. Dent at Abstract. To illustrate, at the instant of handoff, a rapid first resynchronization means temporarily seizes the voice channel in one direction and transmits synchronization information on the seized voice channel. *Id.* Thereafter, the first resynchronization means waits to detect an indication of a successful resynchronization. *Id.* Upon detection of the same, the first resynchronization means ceases transmit of synchronization information and resumes the transmission of speech traffic in the seized voice channel. *Id.*

Even assuming for the sake of argument that Dent describes the above-recited feature of claim 1, Appellant respectfully submits that Dent cannot be combined with Long because Long expressly teaches away from the teachings of Dent. To illustrate and as noted above, Dent teaches a system that requires suspension of data traffics (e.g., voice data) to enable resynchronization (e.g., changing the block counter of mobile device). *See e.g.*, Dent at Abstract, at col. 6, lines 41-58 and col. 14, lines 21-49. In Long's view such a system has several disadvantages. In particular, Long describes that in Dent's system the need for resynchronization can cause downtime on the link and can result in a loss or blockage of huge amount of data. Long at col. 1, lines 28-37. Furthermore, Long describes that the data can be real-time data, where the loss of data is not protected through buffering or protocols. Long at col. 1, lines 38-39. Because of these disadvantages, Long teaches away from the system of Dent and describes a system that seamlessly performs resynchronization, thereby eliminating the downtime associated with Dent's system. *See e.g.*, Long at col. 1, line 65 to col. 2, line 3. That is, Long teaches away from Dent's system by advocating a system that seamlessly updates the resynchronization information instead of halting traffic between the encryptor and the decryptor equipments. *See e.g.*, Long at col. 2, lines 21-28.

For at least the foregoing reasons, Appellant respectfully requests reversal of the rejection of claim 1, along with its dependent claims.

Claim 6 recites a system for communicating Real Time Protocol voice packets between a local and a remote location over an Internet protocol network. The system includes, among other features, a key stream generator for generating a first Real Time Protocol key stream, the stream cipher module employing the first key stream to encrypt the voice packets for forwarding to the remote location, the key stream generator producing a second Real Time Protocol key stream for encrypting the voice packets when the system switches from a first communication parameter to a second communication parameter, each of the first and second parameters being involved in the synchronization of the key stream. Therefore, for at least the reasons presented above with respect to claim 1, Appellant respectfully requests reversal of the rejection of claim 6, along with its dependent claims.

Claim 13 recites a method for securely transmitting Real Time Protocol voice packets from a local to a remote location via a communication network. The method includes, among other steps, a step of generating a second Real Time Protocol key stream for encrypting the voice packets in response to a request to change communication parameters for the same media stream during a communication session. Therefore, for at least the reasons presented above with respect to claim 1, Appellant respectfully requests reversal of the rejection of claim 13, along with its dependent claims.

Claim 19 recites a system for securely transmitting voice packets during a communication session from a local location to a remote location over a communication network. The system includes, among other features, a means for decrypting the encrypted voice packets using the first key stream and a means for generating the first key stream at the remote location in order to decrypt the encrypted voice packets, wherein both means for generating are capable of generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session. Therefore, for at least the reasons presented above with respect to claim 1, Appellant respectfully requests reversal of the rejection of claim 19, along with its dependent claims.

B. Long and Dent fail to describe or suggest all the features of dependent claims 2, 7, and 20.

Claim 2 recites a system, wherein the second key stream is generated when the system switches from a first to a second coder/decoder for compression/decompression of the voice packets. Appellant respectfully submits that neither Long nor Dent describes or suggest the above-recited feature of claim 2. The Office Action asserts that Long describes this feature in column 4, lines 5-35 and column 2,

lines 47-63. Appellant disagrees.

In column 2, lines 47-63, as noted above, Long describes that the key multiplexer (50) switches from key variable 1 to key variable 2 when the KG clock counter (30) reaches a specified switchover value (checked by the comparator (60)). Thereafter, the key variable 2 is used by the key generator (80) to generate a second key. As such, in this section, Long describes generating a second key when a clock counter reaches a specified value and does not describe or otherwise suggest generating a second key stream when a first coder/decoder for compression/decompression of the voice packets changes to a second coder/decoder, as recited in claim 2.

In column 4, lines 5-35, Long describes a method for a seamless cryptographic key system. The described method includes, among other steps, a step of seamlessly updating a cryptographic key for encrypting and decrypting digital data. In particular, the step of seamlessly updating the cryptographic key includes the step of loading key variables into a cryptographic key generator by an interface means to control switch-over of the cryptographic key generator new key variables. Furthermore, the step of seamlessly updating the cryptographic key includes the step of loading a switch-over value into a comparator to control the switch-over. The comparator controls the switching of the multiplexer for both an encrypting subsystem and a decrypting subsystem from a first key variable to a second key variable when the counter reaches a specified state. As such, in this portion too, Long merely describes generating a second key when a clock counter reaches a specified value and does not describe or otherwise suggest generating a second key stream when a first coder/decoder for compression/decompression of the voice packets changes to a second coder/decoder, as recited in claim 2.

For at least the foregoing reasons and those described with respect to claim 1, Appellant respectfully requests reconsideration and withdrawal of the rejection of claim 2.

Claims 7 includes features similar to the above-recited feature of claim 2. Therefore, for at least the reasons presented above with respect to claim 2, Appellant respectfully requests reversal of the rejection of claim 7. In rejecting claim 7, the Office Action points to column 10, line 56 to column 11, line 19 of Dent. In column 10, line 56 to column 11, line 19, Dent describes a symbol detector (126) producing a first output and a second output. The first output is supplied to a module-2 adder (127), which is connected to a 2-burst deinterleaver (128) and a ciphering unit (115). The ciphering unit (115) is used to decipher the encrypted transmitted data by subtracting on a bit-by-bit basis the same keystream used by the transmitter in the base station to encrypt the data. The module-2 adder

(127) and the 2-burst deinterleaver (128) reconstruct the speech data. The deinterleaver (128) is coupled to two channel decoders (129, 130), which decode the encoded speech data.

Although in this portion Dent describes two channel decoders, it does not describe that the alleged two channel decoders are used in generating the second key stream. And, it certainly does not describe or suggest that a change from the alleged first decoder to the alleged second decoder results in generating a key stream. As such, Dent does not describe or suggest a key stream generator for generating a second Real Time Key stream for encrypting the voice packets when the system switches from a first coder/decoder that compresses/decompresses the voice packets to a second coder/decoder that compresses/decompresses the voice packets, as recited in claim 7.

For at least these reasons, Appellant respectfully requests reversal of the rejection of claim 7.

Claim 20 includes features similar to the above-recited features of claim 2, and it was rejected for the same reasons. Therefore, for at least the reasons presented above with respect to claim 2, Appellant respectfully requests reconsideration and withdrawal of the rejection of claim 20.

C. Long, Dent, and Crichton, in the proposed combination, fail to describe or suggest all the features of independent claim 17, and therefore fail to render obvious this claim along with its dependent claim

Claims 17 and 18 were rejected as being unpatentable under 35 U.S.C. § 103(a) over Long, in view of Dent, and further in view of Crichton. Appellant respectfully traverses this rejection for at least the following reasons.

Claim 17 recites a method for securely exchanging voice packets between the multimedia terminal adapters and the gateway. The method includes generating a first Real Time Protocol key stream for encrypting the voice packets and forwarding the voice packets encrypted with the first Real Time Protocol key stream to the gateway. The method also includes generating a second Real Time Protocol key stream for encrypting the voice packets during a communication session in response to a collision detection wherein the multimedia terminal adapters have the same source identifier and forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location. The voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local multimedia terminal adapter and remote multimedia terminal adapter.

Appellant respectfully requests reversal of the rejection of claim 17 because the proposed combination of Long, Dent, and Crichton fails to describe or suggest a method for securely exchanging

voice packets between the multimedia terminal adapters and the gateway, the method including, among other steps, a step of generating a second Real Time Protocol key stream for encrypting the voice packets during a communication session *in response to a collision detection* wherein the multimedia terminal adapters have the same source identifier, as recited in claim 17.

The Office Action asserts that Long describes this feature in column 2, line 47 to column 3, line 5 and column 4, lines 5-35. *See e.g.*, Office Action at page 14, lines 17-19. Appellant disagrees. In column 2, line 47 to column 3, line 5, Long merely describes generating a second key by switching from key variable 1 to key variable 2 when the KG clock counter (30) reaches a specified switchover value. This, at best, describes generating a second key in response to the KG clock counter reaching a particular value and does not describe or suggest generating a second key stream in response to a collision detection, as recited in claim 17.

In column 4, lines 5-35, as noted above, Long describes a method for a seamless cryptographic key system. The described method includes, among other steps, a step of seamlessly updating a cryptographic key for encrypting and decrypting digital data. In particular, this step includes the step of loading key variables into a cryptographic key generator by an interface means to control switch-over of said cryptographic key generator new key variables. As such, in this section too, Long does not describe or suggest a method that includes, among other steps, a step of generating a second Real Time Protocol key stream for encrypting the voice packets during a communication session *in response to a collision detection* wherein the multimedia terminal adapters have the same source identifier, as recited in claim 17.

Dent was cited for an alleged showing that transmitted and received data are voice packets. *See e.g.*, Office Action at page 15, lines 7-117. Crichton was cited for an alleged showing of a gateway. *See e.g.*, Office Action at page 15, lines 18-22. As such, Appellant does not believe that the proposed addition of the subject matter from Dent and Crichton remedy the shortcomings of Long to describe or suggest the above-recited features of claim 17.

For at least the foregoing reasons, Appellant respectfully requests reversal of the rejection of claim 17, along with its dependent claim.

The brief fee of $510 is authorized to be charged to Deposit Account 500417. Please apply any other charges or credits to Deposit Account 500417.

Respectfully submitted,

Date: July 10, 2008

for Lawrence T. Cullen #46,692
Registeration No. 44, 489

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
Phone: 215-323-1797

## Appendix of Claims

1. A system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system comprising:

a local multimedia terminal adapter receiving the voice packets having a time stamp synchronization source operable to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter, the local multimedia terminal adapter comprising,

a local key stream generator for generating a first key stream;

a packet encryptor that encrypts the voice packets using at least a portion of the first key stream to form encrypted voice packets;

the remote multimedia terminal adapter receiving the encrypted voice packets, the remote multimedia terminal adapters further comprising,

a remote key stream generator for generating the first key stream in order to decrypt the encrypted voice packets; and

a packet decryptor decrypting the encrypted voice packets using the first key stream, wherein both key stream generators generate a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session and the packet encryptor and packet decryptor use the second key stream.

2. The system of claim 1 wherein the second key stream is generated when the system switches from a first to a second coder/decoder for compression/decompression of the voice packets.

3. The system of claim 1 wherein the second key stream is generated when a Message Authentication Code algorithm change occurs.

4. The system of claim 1 further comprising a local gateway controller for forwarding the encrypted packets through the Internet protocol network.

5. The system of claim 1 further comprising a remote gateway controller for receiving the encrypted packets from the Internet protocol network and for forwarding encrypted voice packets to

the remote multimedia terminal adapter.

6. A system for communicating Real Time Protocol voice packets between a local and a remote location over an Internet protocol network, the system comprising:

a stream cipher module for encrypting the voice packets; and

a key stream generator for generating a first Real Time Protocol key stream, the stream cipher module employing the first key stream to encrypt the voice packets for forwarding to the remote location, the key stream generator producing a second Real Time Protocol key stream for encrypting the voice packets when the system switches from a first communication parameter to a second communication parameter, each of the first and second parameters being involved in the synchronization of the key stream, wherein the voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local and remote locations.

7. The system of claim 6 wherein the first communication parameter is a first coder/decoder that compresses/decompresses the voice packets, and the second communication parameter is a second coder/decoder that compresses/decompresses the voice packets.

10. The system of claim 6 further comprising a new time tamp sequence generated when the second Real Time Protocol key stream is generated.

11. The system of claim 6 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, "End-End RTP Key Change <N>")

where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session;

F( ) is a one-way pseudo-random function used for the purpose of key derivation;

S is a shared secret which includes a random value shared between the two endpoints and is known only to those two endpoints or a trusted server; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F( ), <N> stands for an ASCII representation of a decimal number, representing a counter.

12. The system of claim 6 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret which includes a random value shared between the two endpoints and is known only to those two endpoints or a trusted server;

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes for the same SSRC value; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F( ), <N> stands for an ASCII representation of a decimal number, representing a counter.

13. A method for securely transmitting Real Time Protocol voice packets from a local to a remote location via a communication network, the method comprising:

generating a first Real Time Protocol key stream for encrypting the voice packets;

forwarding encrypted voice packets to the remote location;

generating a second Real Time Protocol key stream for encrypting the voice packets in response to a request to change communication parameters for the same media stream during a communication session; and

forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location, wherein the voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local and remote locations.

14. The method of claim 13 further comprising reinitializing a time stamp for synchronizing decryption of the voice packets.

15. The method of claim 13 wherein the step of generating a second Real Time Protocol key stream is by re-executing the following key derivation function:

F(S, "End-End RTP Key Change <N>")

where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session;

F( ) is a one-way pseudo-random function used for the purpose of key derivation;

S is a shared secret which includes a random value shared between the two endpoints and is

known only to those two endpoints or a trusted server; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F( ), <N> stands for an ASCII representation of a decimal number, representing a counter.

16. The method of claim 13 wherein the step of generating a second Real Time Protocol key stream is by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret which includes a random value shared between the two endpoints and is known only to those two endpoints or a trusted server;

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F( ), <N> stands for an ASCII representation of a decimal number, representing a counter.

17. In a communication system having a gateway receiving communication sessions from two or more multimedia terminal adapters, a method for securely exchanging voice packets between the multimedia terminal adapters and the gateway, the method comprising:

generating a first Real Time Protocol key stream for encrypting the voice packets;

forwarding the voice packets encrypted with the first Real Time Protocol key stream to the gateway;

generating a second Real Time Protocol key stream for encrypting the voice packets during a communication session in response to a collision detection wherein the multimedia terminal adapters have the same source identifier; and

forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location, wherein the voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local multimedia terminal adapter and remote multimedia terminal adapter.

18. The method of claim 17 wherein the step of generating a second Real Time Protocol key stream is by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret which includes a random value shared between the two endpoints and is known only to those two endpoints or a trusted server;

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F( ), <N> stands for an ASCII representation of a decimal number, representing a counter.

19. A system for securely transmitting voice packets during a communication session from a local location to a remote location over a communication network, the system comprising:

a means for generating a first key stream at the local location;

a means for encrypting the voice packets using at least a portion of the first key stream to form encrypted voice packets;

a means for forwarding the encrypted voice packets from the local location to the remote location;

a means for generating the first key stream at the remote location in order to decrypt the encrypted voice packets; and

a means for decrypting the encrypted voice packets using the first key stream, wherein both means for generating are capable of generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session, wherein the voice packets have a time stamp synchronization source operable to synchronize cryptographic operations between said local and remote locations.

20. The system of claim 19 wherein the second key stream is generated when the system switches from a first to a second coder/decoder for compression/decompression of the voice packets.

21. The system of claim 19 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, "End-End RTP Key Change <N>")

where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session;

F( ) is a one-way pseudo-random function used for the purpose of key derivation;

S is a shared secret which includes a random value shared between the two endpoints and is known only to those two endpoints or a trusted server and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F( ), <N> stands for an ASCII representation of a decimal number, representing a counter.

22. The system of claim 19 wherein the second key stream is generated by re-executing the following key derivation function:

F(S, SSRC, "End-End RTP Key Change <N>") where:

S is a shared secret which includes a random value shared between the two endpoints and is known only to those two endpoints or a trusted server;

SSRC is the synchronization source session identifier;

N is the counter of the number of key changes; and

"End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F( ), <N> stands for an ASCII representation of a decimal number, representing a counter.

23. The system of claim 19 further comprising a means for synchronizing the voice packets.

## Evidence Appendix

None.

## Related Proceedings Appendix

None.